Lecture notes on rewriting theory
Lecture 6
Frédéric Blanqui (INRIA)
19 September 2016, last revised on 21 October 2020

1 Modularity of confluence

Let \( V \) be a set of variables and \( F_a (a \in \{1, 2\}) \) be two sets of function symbols. Let \( T_a = \mathcal{T}(F, V) \) and \( T = \mathcal{T}(F, V) \) where \( F = F_1 \cup F_2 \). You can think of 1 and 2 as colors (e.g. blue and red). A term \( t \in T_a \) is said to be of color \( a \). Let \( \overline{1} = 2 \) and \( \overline{2} = 1 \), the function swapping the colors.

Let \( R_a (a \in \{1, 2\}) \) be a set of rewriting rules on \( T_a \), whose left-hand sides are not variables, and \( R = R_1 \cup R_2 \). Then, let \( \rightarrow_{R_a} (\rightarrow_{\overline{a}} \text{ resp.}) \) be the smallest rewrite relation on \( T_a \) (\( T \) resp.) containing \( R_a \), and \( \rightarrow \) be the smallest rewrite relation on \( T \) containing \( R \).

A property \( P \) on rewrite relations is said to be modular if \( P(\rightarrow) \) holds whenever both \( P(\rightarrow_{R_1}) \) and \( P(\rightarrow_{R_2}) \) hold.

Note that the case \( R_2 = \emptyset \) is already interesting as it corresponds to signature extension.

We have already seen that termination is not modular, even if \( F_1 \) and \( F_2 \) are disjoint. (Termination is preserved by signature extension though, the proof of which is not completely trivial.)

In this section, we are going to prove that confluence is modular if \( F_1 \) and \( F_2 \) are disjoint.

We first introduce some definitions to reason about the different color layout of a term of \( T \).

Let \( C = \mathcal{T}(F \cup \{\Box\}, V) \) be the set of multi-contexts. A multi-context \( C \) is of color \( a \) if \( C \in C_a = \mathcal{T}(F_a \cup \{\Box\}, V) \). Given a multi-context \( C \) where the occurrences of \( \Box \) are at positions \( p_1, \ldots, p_n \), and \( n \) terms \( t_1, \ldots, t_n \), let \( C[t_1, \ldots, t_n] \) be the term obtained by replacing in \( C \) the \( i \)-th occurrence of \( \Box \) by \( t_i \), for every \( i \in \{1, \ldots, n\} \).

For every term \( t \in \mathcal{T}(F, V) \) headed by a function symbol of color \( a \), there is a unique pair \( (C, t_1 \ldots t_n) \) where \( C \) is a multi-context of color \( a \) and \( t_1 \ldots t_n \) is a possibly empty sequence of terms headed by function symbols of color \( \overline{a} \) such that \( t = C[t_1, \ldots, t_n] \). \( C \) is called the cap of \( t \), \( cap(t) \), and \( t_1 \ldots t_n \) the direct aliens of \( t \), \( aliens(t) \).
We extend this notion of cap and aliens to variables by taking $\text{cap}(x) = x$ and $\text{aliens}(x) = []$ (the empty list).

Let $t \rightarrow^c u$ (cap reduction) if $t \xrightarrow{\text{cap}} u$ and $p \in \text{Pos}(\text{cap}(t))$, and $t \rightarrow^a u$ (alien reduction) if $t \xrightarrow{\text{cap}} u$ and $p \notin \text{Pos}(\text{cap}(t))$.

- If $t \rightarrow^c u$ then either
  - $u \in \text{aliens}(t)$, or
  - $\text{cap}(t) \rightarrow \text{cap}(u)$ and $\text{aliens}(u) \subseteq \text{aliens}(t)$ (each alien of $u$ is an alien of $t$).
- If $t \rightarrow^a u$ and $\text{aliens}(t) = [t_1, \ldots, t_n]$ then there is $i$ and $t'_i$ such that $t_i \rightarrow t'_i$ and $u = \text{cap}(t)[t_1, \ldots, t'_i, \ldots, t_n]$ (note that $\text{cap}(u) \neq \text{cap}(t)$ if $t_i$ and $t'_i$ are headed by symbols of different colors).

We recursively define the rank of a term as the maximum number of monochrome layers composing it by:

$$\text{rk}(t) = 1 + \max\{\text{rk}(u) \mid u \in \text{aliens}(t)\}$$

with $\max\emptyset = 0$.

First note that, because rules are monochrome, rewriting does not increase the rank:

**Lemma 1** If $t \rightarrow u$, then $\text{rk}(t) \geq \text{rk}(u)$.

A rewrite step $t \rightarrow u$ is destructive at level 1 if $u$ is a variable or else $t$ and $u$ have root symbols of different colors (hence $u$ is an alien of $t$).

A rewrite step $t \rightarrow u$ is destructive at level $n+1$ if $\text{aliens}(t) = [t_1, \ldots, t_k, \ldots, t_n]$, $u = \text{cap}(t)[t_1, \ldots, t'_k, \ldots, t_n]$ and $t_k \rightarrow t'_k$ is destructive at level $n$.

A term $t$ is stable if there are no reduction sequence starting from $t$ containing a destructive step.

A term $t$ is alien-stable if all its aliens are stable.

We define the set $S(t)$ of special subterms of a term $t$ recursively by:

$$S(t) = \{t\} \cup \bigcup\{S(u) \mid u \in \text{aliens}(t)\}$$

Let $t \Rightarrow u$ (collapsing reduction) iff there are $C$, $s \in S(t)$ and $s'$ such that $t = C[s]$, $s \rightarrow^* s'$, $u = C[s']$, and either $s' \in \mathcal{V}$ or else root(s) and root(s') have different colors.

Note that $t$ is stable iff $t$ is in normal form wrt $\Rightarrow$.

**Lemma 2** $\Rightarrow$ terminates.

Proof. Let $\|t\|$ be the empty multiset if $t$ is a variable, and the multiset $\{|\text{rk}(s) \mid s \in S(t)\}$ otherwise. We prove that $\|t\|_{(\text{max})} \leq \|t'\|$ whenever $t \Rightarrow t'$. Note that $s \rightarrow^+ s'$. Let $p$ be the position of $\square$ in $C$. $S(t')$ can be obtained from $S(t)$ by replacing every term containing $s$ along a suffix $q$ of $p$, say $D[s]_q$, by $D[s']_q$, and by replacing the elements of $S(s)$ by those of
In the first case, we have $\text{Lemma 3} \rightarrow C$ ordering terms, every equivalence class $\tau$ is ever $t$.

By assumption, there is $\text{equivalence class of } t_n > \text{induction on } n$. For $\text{symmetric by definition.}$ It is also transitive. Indeed, assume that $t$ is a function $\hat{t}$ thanks to the previous property. We have $t \rightarrow \tau$ for all $t, u \in \text{Lemma 4}$ Every finite set $\tau$ and confluent, there is $\text{Then, there are } \tau$ and $\text{for all } v \in S(s'), rk(s) > rk(s')$ and, for all $v \in S(s'), rk(s) > rk(s') \geq rk(v)$. Therefore, $\|t\| > \text{mult} \|t'\|$. $\blacksquare$

Hence, every term is reducible to a stable term.

We now check that cap reduction is confluent:

**Lemma 3** $\rightarrow_{a}^{\tau}$ is confluent.

Proof. Given a term $t$ whose cap is $C$ and whose aliens are $t_1, \ldots, t_n$, let $|t| = C[x_1, \ldots, x_n]$ where $x_1, \ldots, x_n$ are fresh variables such that $x_i = x_j$ whenever $t_i = t_j$, and let $\sigma$ be the substitution mapping $x_i$ to $t_i$ (it is well defined thanks to the previous property). We have $t = |t| \sigma$. Moreover, if $t \rightarrow_{a} u$, then $|t| \rightarrow_{a} |u|$. Therefore, $\rightarrow_{a}^{\tau}$ is confluent since $\rightarrow_{a}$ so is. $\blacksquare$

A set $M$ of confluent terms is representable by some set $N$ of terms if there is a function $\tau: M \rightarrow N$ such that:

- for all $t \in M$, $t \rightarrow^{\tau} \hat{t}$;
- for all $t, u \in M$, $\hat{t} = \hat{u}$ whenever $t \downarrow u$.

**Lemma 4** Every finite set $M$ of confluent terms is representable by a set $\hat{M}$.

Proof. First note that $\downarrow$ is an equivalence relation on $M$. It is reflexive and symmetric by definition. It is also transitive. Indeed, assume that $t_1 \downarrow t_2 \downarrow t_3$. Then, there are $u_1$ and $u_2$ such that $t_1, t_2 \rightarrow^{*} u_1$ and $t_2, t_3 \rightarrow^{*} u_2$. Since $t_2$ is confluent, there is $u_1$ such that $u_1, u_2 \rightarrow^{*} v_1$. Therefore, $t_1 \downarrow t_3$.

More generally, given $n \geq 2$ confluent terms $t_1, \ldots, t_n$ such that $t_1 \downarrow \cdots \downarrow t_n$, there is a term $\tau(t_1, \ldots, t_n)$ such that, for all $1 \leq i \leq n$, $t_i \rightarrow^{*} \tau(t_1, \ldots, t_n)$, by induction on $n$. For $n = 2$, this is immediate by assumption. So, assume that $n > 2$. By induction hypothesis, for all $1 \leq i < n$, $t_i \rightarrow^{*} u = \tau(t_1, \ldots, t_{n-1})$. By assumption, there is $v$ such that $t_{n-1}, t_n \rightarrow^{*} v$. By confluence of $t_{n-1}$, there is $w$ such that $u, v \rightarrow^{*} w$. For all $1 \leq i \leq n$, $t_i \rightarrow^{*} w$. Therefore, we can take $\tau(t_1, \ldots, t_n) = w$.

Now, $M$ being finite, every equivalence class modulo $\downarrow$ is finite. By well-ordering terms, every equivalence class $C$ can be mapped to the ordered list $l(C)$ of all the terms in $C$. To conclude, it suffices to take $N = M$ and $\hat{t} = \tau(l(|t|))$ where $|t|$ is the equivalence class of $t$. $\blacksquare$

**Lemma 5** $\rightarrow$ is confluent on alien-stable terms.
Proof. We prove that every alien-stable term \( t \) is confluent, by induction on the rank of \( t \).

Terms of rank 1 are monochrome, hence confluent.

Assume that \( t = t_0 \to t_1 \to \ldots \to t_p \) and \( t = u_0 \to u_1 \to \ldots \to u_q \).

Wlog we can assume that root(\( t \)) is of color 1.

Let \( M \) be the set of all the maximal special subterms of some \( t_i \) or \( u_i \) whose root symbol is of color 2.

Every element \( s \) of \( M \) has a rank smaller than the rank of \( t \). First every \( t_i \) and \( u_i \) has a rank smaller or equal to the rank of \( t \). Wlog we can assume that \( s \) is a subterm of \( t_i \). If root(\( t_i \)) is of color 1, then \( rk(t) \geq rk(t_i) > rk(s) \). If root(\( t_i \)) is of color 2, then there is \( j < i \) such that root(\( t_j \)) if of color 1 and root(\( t_{j+1} \)) is of color 2. Hence, \( t_{j+1} \in \text{aliens}(t_j) \) and \( rk(t) \geq rk(t_j) > rk(t_{j+1}) \geq rk(t_i) \).

So, by induction hypothesis, every element of \( M \) is confluent.

Let \( M \) be a set representing \( M \).

Given a term \( v \), let \( \bar{v} \) be \( v \) with all its subterms \( s \in M \) replaced by \( \hat{s} \).

We prove that, if \( a \to b \) is \( t_i \to t_{i+1} \) or \( u_i \to u_{i+1} \), then \( \hat{a}(\to^{i}_\hat{\eta})^{\hat{\epsilon}} b \):

- If root(\( a \)) is of color 1.
  - If \( a \to^{\epsilon} b \). Then, \( a \to^{\hat{\eta}} b \) and \( \hat{a} \to^{\hat{\eta}} \hat{b} \).
  - Otherwise \( a \to^{a} b \), that is, \( a = C[a_1, \ldots, a_k, \ldots, a_n] \), \( a_k \to a'_k \) and \( b = C[a_1, \ldots, a'_k, \ldots, a_n] \). Since \( a_k, a'_k \in M \) (by stability) and \( a_k \downarrow a'_k \), \( \hat{a}_k = \hat{a}'_k \).
    Therefore, \( \hat{a} = \hat{b} \).

- Otherwise root(\( a \)) is of color 2. Then a destructive step \( a' \to b' \) occurred before, with root(\( a' \)) of color 1, \( b' \in \text{aliens}(a') \) and root(\( b' \)) of color 2. Since \( t \) is alien-stable, \( b' \) is stable. So root(\( b \)) is of color 2. Since \( a, b \in M \) and \( a \downarrow b \), we have \( \hat{a} = \hat{b} \) and \( \hat{a} = \hat{b} \).

Therefore, \( \hat{t}(\to^{i}_\hat{\eta})^{\hat{\epsilon}} t_p, \hat{u}_i \) and \( t_p \downarrow u_q \) since \( \to^{i}_\hat{\eta} \) is confluent and \( t_p \to^{*} \hat{t}_p \) and \( u_q \to^{*} \hat{u}_q \).

A witness of a term \( t \) whose aliens are \( t_1, \ldots, t_n \) is an alien-stable term of the form \( \text{cap}(t)[u_1, \ldots, u_n] \) with, for all \( i, t_i \to^{*} u_i \) and, for all \( i, j, u_i = u_j \) whenever \( t_i = t_j \).

**Lemma 6** Every term \( t \) reduces to a witness of \( t \), written \( \hat{t} \).

Proof. Assume that the aliens of \( t \) are \( t_1, \ldots, t_n \). For each \( i \), let \( u_i \) be a normal form of \( t_i \) wrt \( \Rightarrow \), such that \( u_i = u_j \) whenever \( t_i = t_j \). Then, let \( \hat{t} = \text{cap}(t)[u_1, \ldots, u_n] \). We have \( t \to^{*} \hat{t} \) since \( \Rightarrow \subseteq \to^{*} \). The aliens of \( \hat{t} \) are subterms of the terms \( u_1, \ldots, u_n \) which are stable. Therefore, they are stable too, and \( \hat{t} \) is alien-stable.

**Lemma 7** If \( t \to u \) and the aliens of \( t \) are confluent, then \( \hat{t} \downarrow \hat{u} \).

Proof. Assume that aliens(\( t \)) = \( t_1, \ldots, t_n \) and \( \hat{t} = \text{cap}(t)[u_1, \ldots, u_n] \).
• If $t \rightarrow^c t_i$. We have $\dot{t} \rightarrow u_i \downarrow \dot{t}_i$ since $t_i \rightarrow^* u_i, \dot{t}_i$ and $t_i$ is confluent.

• If $t \rightarrow^c u \notin \text{ aliens}(t)$. Then, $u = \text{ cap}(u)[t_{k_1}, \ldots, t_{k_p}], \dot{u} = \text{ cap}(u)[v_{k_1}, \ldots, v_{k_p}]$ and $\dot{t} \rightarrow \text{ cap}(u)[u_{k_1}, \ldots, u_{k_p}] \downarrow \dot{u}$ since, for all $i$, $t_{k_i} \rightarrow^* u_{k_i}, v_{k_i}$ by definition of witness, and $t_{k_i}$ is confluent.

• Otherwise $t \rightarrow^a u = \text{ cap}(t)[t_1, \ldots, t'_{k}, \ldots, t_n]$ with $t_k \rightarrow t'_k$. Then, $\dot{u} = \text{ cap}(t)[v_1, \ldots, v_{k}, \ldots, v_n]$. For all $i$, $u_i \downarrow v_i$ since $t_i \rightarrow^* u_i, v_i$ by definition of witness and $t_i$ is confluent. Therefore, $t \downarrow \dot{u}$.

We can now complete of proof of confluence of $\rightarrow$ on arbitrary terms:

**Theorem 1** If $\rightarrow_1$ is confluent on $\mathcal{T}_1$, $\rightarrow_2$ is confluent on $\mathcal{T}_2$, and $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$, then $\rightarrow$ is confluent on $\mathcal{T}$.

**Proof.** By induction on the rank. The case of rank 1 is immediate.

Assume that $t = t_0 \rightarrow \ldots \rightarrow t_p, u = u_0 \rightarrow \ldots \rightarrow u_q$, and $\text{ rank}(t) > 1$. For all $i$, $t_i \rightarrow^* \dot{t}_i$ and $u_i \rightarrow^* \dot{u}_i$. By induction hypothesis, the aliens of $t_i$ and $u_i$ are confluent. Hence, for all $i$, $t_i \downarrow t_{i+1}$ and $u_i \downarrow u_{i+1}$. But the terms $\dot{t}_i$ and $\dot{u}_i$ are alien-stable and thus confluent. Therefore, $t_p \downarrow u_q$. ■